# From oscillatory integrals to complete exponential sums

Wright, J 2011, 'From oscillatory integrals to complete exponential sums' Mathematical Research Letters, vol 18, no. 2, pp. 231-250.

# FROM OSCILLATORY INTEGRALS TO COMPLETE EXPONENTIAL SUMS

JAMES WRIGHT

ABSTRACT. In [8], Phong and Stein establish a sharp and stable bound for (one dimensional) scalar oscillatory integrals with a polynomial phase $\phi$ in terms of root clusters of the derivative $\phi'$. In this note we prove an analogous result for complete exponential sums. When one considers only singleton clusters, the corresponding estimate for exponential sums was established by Loxton and Vaughan in [5]. Considering all possible clusters containing a particular root allows one to obtain bounds for exponential sums which are stable under perturbations of the phase.

## 1. INTRODUCTION

There is a striking similarity between certain problems in euclidean harmonic analysis, for example the Fourier restriction problem or establishing smoothing estimates for Radon-like transforms, and the corresponding problem in the setting of the ring of integers modulo $n$, $\mathbb{Z}/n\mathbb{Z}$. Such problems have been extensively studied in the setting of finite fields (see for example, [6] and [1]) and have served as good models for the original euclidean problems. However a difference one finds when passing from the euclidean setting to the finite field setting is the lack of scales at one's disposal. Moving from finite fields, say $\mathbb{Z}/p\mathbb{Z}$ where $p$ is prime, to the ring $\mathbb{Z}/n\mathbb{Z}$ for general $n$, the various divisors of $n$ serve as different scales. By introducing an appropriate "absolute value" or "norm" for integers mod $n$, euclidean scaling arguments can be made to work in this setting and one sees that euclidean problems are modeled more closely in $\mathbb{Z}/n\mathbb{Z}$ than in the finite field setting.

In this note we continue exploring this similarity (see also [10], [3], [11] and [12]) in the context of estimates for oscillatory integrals in the euclidean setting on the one hand and estimates for complete exponential sums in elementary number theory on the other hand. More specifically we will establish an analogous estimate for exponential sums of a very useful and sharp estimate for oscillatory integrals due to Phong and Stein [8]: suppose that $\phi \in \mathbb{R}[X]$ is polynomial with real coefficients whose derivative $\phi'(x) = a_0 \prod (x - z_j)^{e_j}$ has $m$ distinct roots $\{z_1, \ldots, z_m\}$. By a *root cluster* $\mathcal{C}$ we simply mean a subset $\mathcal{C} \subset \{z_1, \ldots, z_m\}$ of the roots and we write $S(\mathcal{C}) = \sum_{j: z_j \in \mathcal{C}} e_j$ as the number of roots in this cluster, counted with multiplicities.

1991 *Mathematics Subject Classification.* 11A07, 11L07, 11L40, 42B20.
The author was supported in part by an EPSRC grant.

Given a real parameter $\lambda$, a root $z_j$ of $\phi'$ and root cluster $\mathcal{C}$ containing $z_j$, we define

$$E_\lambda(z_j;\mathcal{C}) \;=\; \Big[\frac{|\lambda|^{-1}}{|a_0\prod_{z_k\notin\mathcal{C}}(z_j-z_k)^{e_k}|}\Big]^{1/[S(\mathcal{C})+1]}$$

which will arise as a *cluster estimate* for the oscillatory integral

$$I_\lambda \;=\; \int_a^b e^{2\pi i\lambda\phi(x)}\psi(x)\,dx;$$

here $\psi$ is smooth and has compact support if either endpoint $a$ or $b$ is infinite. In [8] the following estimate for $I_\lambda$ was proved:

$$|I_\lambda| \;\le\; C\max_{1\le j\le m}\min_{z_j\in\mathcal{C}} E_\lambda(z_j;\mathcal{C}) \tag{1}$$

where the minimum is taken over all root clusters $\mathcal{C}$ containing $z_j$ and $C$ depends only on the degree $d=\sum e_j$ of $\phi'$, $\|\psi\|_{L^\infty}$ and $\|\psi'\|_{L^\infty}$. This estimate is stable under perturbations of the phase $\phi$. It is also a sharp estimate when all the roots of $\phi'$ are real. When a root $z_j$ is complex, there is an improved *cluster estimate* $E'_\lambda(z_j;\mathcal{C})$ (smaller than $E_\lambda(z_j;\mathcal{C})$), giving rise to a better bound in (1). This uses the fact that when $z_j=a_j+ib_j$ is complex, the absolute value $|\cdot|$ of the factor $(x-z_j)$ in $\phi'$ has the bound $|x-z_j|\sim\max(|x-a_j|,|b_j|)$, and in particular the uniform bound from below $|x-z_j|\ge|b_j|$ holds which can be exploited in the oscillatory integral estimate for $I_\lambda$.

When we pass to exponential sums where our polynomial phase $\phi\in\mathbb{Z}[X]$ now has coefficients in the integers $\mathbb{Z}$, non-archimedean absolute values $|\cdot|'$ on the integers $\mathbb{Z}$ will play the analogous role of the archimedean absolute value $|\cdot|$ on the reals $\mathbb{R}$. Unlike the archimedean case, where $|\cdot|$ extends uniquely to $\mathbb{C}$ with the above uniform bounds on the factors $|x-z_j|$, the analogous bounds for $|x-z_j|'$ for extensions of non-archimedean absolute values $|\cdot|'$ to fields $K$ containing the roots of $\phi'$ do not hold (or at least are not easy to come by) uniformly for $x\in\mathbb{Z}$. Nevertheless we will prove an analogue of (1) for complete exponential sums.

Let us begin with a polynomial $\phi\in\mathbb{Z}[X]$ and consider the exponential sum

$$S(\phi;N) \;=\; \frac{1}{N}\sum_{x\bmod N} e^{2\pi i\phi(x)/N}$$

where $N\in\mathbb{N}$ is a fixed positive integer. Due to the multiplicative nature of $S(\phi;N)$, the study of these sums can be reduced to understanding $S(\phi;N)$ when $N=p^\alpha$ is a power of a fixed prime $p$. This allows us to employ a single absolute value in our analysis, the so-called $p$-adic absolute value $|\cdot|$, defined on integers $x\in\mathbb{Z}$ by $|x|=p^{-t}$ where $p^t$ appears in the prime factorization of $x$. Henceforth $|\cdot|$ will either denote the $p$-adic absolute value or some other absolute value, archimedean or non-archimedean (we also call a non-archimedean absolute value a *valuation*), the context will always be clear. Furthermore, it is sometimes convenient to use additive notation for valuations; in the case of the $p$-adic valuation $|\cdot|$ on $\mathbb{Z}$, this is defined as the nonnegative integer $\mathrm{ord}_p(x)$ so that $|x|=p^{-\mathrm{ord}_p(x)}$. For our sum $S(\phi;p^\alpha)$, it is the roots of the derivative $\phi'(x)=a_0\prod(x-\xi_j)^{e_j}$ which play a key role; here $\{\xi_1,\ldots,\xi_m\}$ enumerate the distinct roots of $\phi'$, lying in some finite field extension $K$ of the $p$-adic field $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to the $p$-adic valuation $|\cdot|$. The $p$-adic valuation $|\cdot|$ or $\mathrm{ord}_p$ extends uniquely to a valuation

on $K$; we write this extension as $|\cdot|$ and $\mathrm{ord}_p$ in the multiplicative and additive form respectively. Therefore, with respect to this extension, the *cluster estimate* $E_{p^{-\alpha}}(\xi_j;\mathcal{C})$ makes sense in this discrete setting;

$$E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \;:=\; \Big[\frac{p^{-\alpha}}{|a_0\prod_{\xi_k\notin\mathcal{C}}(\xi_j-\xi_k)^{e_k}|}\Big]^{1/[S(\mathcal{C})+1]} \tag{2}$$

where $\mathcal{C}\subset\{\xi_1,\dots,\xi_m\}$ is a fixed root cluster of $\phi'$ containing $\xi_j$. The absolute value $|\cdot|$ is now non-archimedean and $p^{-\alpha}$ plays the role of the real parameter $\lambda$ (here we note $|p^{-\alpha}|=p^{\alpha}$).

Our main result is the following estimate.

**Theorem 1.1.** *For any polynomial $\phi\in\mathbb{Z}[X]$ of degree at least 2, we have*

$$|S(\phi;p^{\alpha})| \;\le\; mp^2\max_{1\le j\le m}\min_{\xi_j\in\mathcal{C}}E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \tag{3}$$

*where the minimum is taken over all all root clusters $\mathcal{C}$ containing $\xi_j$.*

### 1.2. **Remarks.**

- As we will see, the proof of Theorem 1.1 is elementary and conceptually simple. This is the most significant feature of the result. To prove (3) it suffices to assume that $p^2\max_j\min_{\mathcal{C}}E_{p^{-\alpha}}(\xi_j;\mathcal{C})<1$; otherwise there is nothing to prove. We will see that this assumption forces $\alpha\ge 2$ and so there will be no need to appeal to the estimates of A. Weil for exponential sums over finite fields.
- Improvements on the factor $mp^2$ are possible. A slight variant of the argument establishing (3), now using the estimates of A. Weil, easily shows that $mp^2$ can be replaced by $2(d-1)^2p^{3/2}$. See Section 6 where further improvements are discussed. It is likely that the factor $mp^2$ can be replaced by some constant $C$ depending only on the degree of $\phi$, at least for large $p$. This is the case if the minimum $\min E_{p^{-\alpha}}(\xi_j;\mathcal{C})$ in (3) over all clusters $\mathcal{C}$ containing $\xi_j$ is replaced by $E_{p^{-\alpha}}(\xi_j;\{\xi_j\})$, thus restricting ones attention to just singleton clusters (a result due to Loxton and Vaughan, [5]; see the last remark below), or if one considers only the biggest root cluster consisting of all roots of $\phi'$ (essentially reducing to a classical result of Hua). We do not make any effort here to optimise the estimate.
- The classical estimate of Hua [2] mentioned above is the following. If $\phi(x)=b_dx^d+\cdots+b_1x$, then $|S(\phi;p^{\alpha})|\le C_dp^{-\alpha/d}$ whenever $gcd(b_d,\dots,b_1,p^{\alpha})=1$. To see how this estimate is related to (3), suppose $\phi'(x)=a_0\prod(x-\xi_j)^{e_j}$ as before and observe that for each $1\le j\le m$,

  $$\min_{\xi_j\in\mathcal{C}}E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \;\le\; E_{p^{-\alpha}}(\xi_j;\mathcal{C}_g) \;=\; p^{-\alpha/d}$$

  whenever $p$ does not divide the top coefficient $a_0$. Here $\mathcal{C}_g=\{\xi_1,\dots,\xi_m\}$. Now if $p$ divides $a_0$ but does not divide the next coefficient, then a simple combinatorial argument shows that $\min_{\xi_j\in\mathcal{C}}E_{p^{-\alpha}}(\xi_j;\mathcal{C})\le p^{-\alpha/(d-1)}\le p^{-\alpha/d}$ for each $j$. Interestingly this combinatorial reasoning continues to hold *only* if $p$ does not divide a top coefficient $a_k$ for some $k\le(d-1)/2$, showing that $\min_{\xi_j\in\mathcal{C}}E_{p^{-\alpha}}(\xi_j;\mathcal{C})\le p^{-\alpha/d}$ for each $j$ in these cases. For

$k > (d-1)/2$, not only does the reasoning break down but the estimate $\max_j \min_{\xi_j \in \mathcal{C}} E_{p^{-\alpha}}(\xi_j; \mathcal{C}) \leq p^{-\alpha/d}$ is false in general. Nevertheless the proof of Theorem 1.1 below shows that (3) holds if the maximum in (3) is taken only over those $1 \leq j \leq m$ such that $|\xi_j| \leq 1$. In this case one can show

$$\max_{j:|\xi_j|\leq 1} \min_{\xi_j \in \mathcal{C}} E_{p^{-\alpha}}(\xi_j; \mathcal{C}) \ \leq \ p^{-\alpha/d}$$

whenever $gcd(b_d, \dots, b_1, p^\alpha) = 1$ which corresponds to the classical Hua estimate. See the final section, Section 7.

- To establish the estimate (3), we will begin by writing the sum $S(\phi; p^\alpha)$ as an "oscillatory integral" over the compact group $\mathbb{Z}_p$ of $p$-adic integers. This will allow us to follow closely a euclidean argument establishing (1). We present this argument in the Section 2 where we will see how the oscillatory integral $I_\lambda$ is efficiently controlled by a certain sublevel set of $\phi'$. In our discrete setting this translates to controlling the exponential sum $S(\phi; p^\alpha)$ by the number of solutions to a certain polynomial congruence given by $\phi'$.

  The principle of controlling $S(\phi; p^\alpha)$ by $N(\phi'; p^s) := p^{-s}\#\{\phi' \equiv 0 \bmod p^s\}$, the normalised number of solutions to the polynomial congruence $\phi' \equiv 0 \mod p^s$, for some choice of $s$ is well known and has been used previously. For instance if $\alpha = 2\beta \geq 2$ is an even integer, then $|S(\phi, p^\alpha)| \leq N(\phi'; p^\beta)$ is an elementary estimate and has been used in [7] and [4]. Our use of this principle lies deeper, the choice of $s$ not only depends on $\alpha$ but also on the roots of $\phi'$. See Section 5. We emphasise that the implementation of the principle is nevertheless elementary.
- The estimate (3) in Theorem 1.1 can be rewritten using the additive form $\mathrm{ord}_p$ of the extension to $K$ of the $p$-adic valuation on $\mathbb{Z}$. Let

$$\delta_p(\xi_j; \mathcal{C}) \ := \ \mathrm{ord}_p\big(a_0 \prod_{k:\xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k}\big)$$

  and

$$\theta_j \ = \ \theta_j(\alpha) \ := \ \max_{\xi_j \in \mathcal{C}} \frac{(\alpha - \delta_p(\xi_j; \mathcal{C}))}{S(\mathcal{C}) + 1}$$

  where the maximum is taken over all root clusters $\mathcal{C}$ containing the root $\xi_j$. Then (3) can be reformulated as

$$|S(\phi; p^\alpha)| \ \leq \ m p^{-\min_j [\theta_j(\alpha)]+2}. \tag{4}$$

  If one considers only singleton clusters $\mathcal{C} = \{\xi_j\}$, then $p^{-\min_j \theta_j(\alpha)} \leq p^{-(\alpha-\delta)/(e+1)}$ where $\delta = \max_j \delta_p(\xi_j; \{\xi_j\})$ and $e = \max_j e_j$. If $d$ is the degree of $\phi$, then the estimate

$$|S(\phi; p^\alpha)| \ \leq \ (d-1) p^{-(\alpha-\delta)/(e+1)} \tag{5}$$

  when $p > d$ was established in [5]. Considering only singleton clusters has the disadvantage that the corresponding bound can be unstable; the estimate (5) can change drastically if two close by roots of $\phi'$ are perturbed to coincide. This is rectified by considering all possible clusters containing a particular root.
- Nevertheless it is likely that the argument in [5] to prove (5) can be used to establish the estimate (3) or (4), even with improvements on the factor $p^2$. We were unaware of [5] when Theorem 1.1 was proved and we thank

Trevor Wooley for pointing out this reference to us. The argument we give follows a harmonic analysts perspective and therefore hopefully accessible to non-experts in number theory. We refer the reader to [5] for further background and references.

1.3. **Examples.** In many cases root clusters with more than a single element can realise the *max min* occuring in the estimate (3) of Theorem 1.1. For instance if $\phi'(x) = \prod(x-\xi_j)^{e_j}$ and $\alpha$ is small in the sense that

$$p^{\alpha/d} \ \leq \ \max_{1\leq j\leq m} \prod_{k\neq j} |\xi_j - \xi_k|^{e_k},$$

then the root cluster $\mathcal{C}_g = \{\xi_1, \ldots, \xi_m\}$ containing all the roots determines the estimate; namely, $\max\min E_{p^{-\alpha}}(\xi_j;\mathcal{C}) = p^{-\alpha/d}$ where $d = \text{degree}(\phi)$. This is the case corresponding to the exponential sum estimate due to Hua discussed above.

However, fixing the roots of $\phi'$ and letting $\alpha$ tend to $\infty$, it is the singleton root clusters which dictate the estimate and the behaviour of the exponential sum. See [5] where several examples are given and discussed in this situation. On the other hand when $\alpha$ is small or in a middle range with respect to root separations measured in terms of the $p$-adic valuation (or thinking of $\alpha$ as being fixed and perturbing the roots of $\phi'$ so that they "cluster" near a given root), then larger sized root clusters can dominate.

For instance consider the example

$$\phi'(x) = a(x-\xi_1)^{e_1}(x-\xi_2)^{e_2}(x-\xi_3)^{e_3}$$

of a polynomial $\phi \in \mathbb{Z}[X]$ of degree $d = e_1+e_2+e_3+1$ with three distinct roots $\xi_1, \xi_2$ and $\xi_3$. Suppose that the root $\xi_1$ is equidistant from the roots $\xi_2$ and $\xi_3$; that is,

$$s \ := \ \text{ord}_p(\xi_1-\xi_2) \ = \ \text{ord}_p(\xi_1-\xi_3).$$

Then necessarily the distance between $\xi_2$ and $\xi_3$ must be shorter; that is, $t \ := \ \text{ord}_p(\xi_2-\xi_3) \geq s$. Let's fix the multiplicities of the roots so that $e_2 \leq e_1 \leq e_3$.

In this case, $\delta = \max_j \delta_j(\xi_j;\{\xi_j\}) = \tau + e_1 s + e_3 t$ where $\tau = \text{ord}_p(a)$ and the estimate (5) (if $p > d$) becomes

$$|S(\phi;p^\alpha)| \ \leq \ (d-1)p^{-(\alpha-\tau-e_1 s-e_3 t)/(e_3+1)}.$$

As $t$ gets large (equivalently, as $\xi_3 \to \xi_2$), this estimate blows up and in the limit we arrive at a phase $\tilde{\phi}$ with $\tilde{\phi}'(x) = a(x-\xi_1)^{e_1}(x-\xi_2)^{e_*}$ where $e_* = e_2+e_3$. If instead we consider all clusters containing a particular root, then it is the cluster $\mathcal{C} = \{\xi_2, \xi_3\}$ which plays the key role and we have

$$\min_{1\leq j\leq 3} \theta_j(\alpha) \ = \ \theta_2(\alpha) \ = \ (\alpha - \delta_p(\xi_2;\mathcal{C}))/(S(\mathcal{C})+1) \ = \ (\alpha-\tau-se_1)/(e_2+e_3+1)$$

when $ds \leq \alpha-\tau \leq se_1 + t(e_2+e_3+1)$. The estimate (3) or (4) is then

$$|S(\phi;p^\alpha)| \ \leq \ 3p^2 p^{-(\alpha-\tau-se_1)/(e_2+e_3+1)}.$$

In the limit, for $\tilde{\phi}$, it is the cluster $\tilde{\mathcal{C}} = \{\xi_2\}$ which now dominates and we have

$$\min_{1\le j\le 2} \tilde{\theta}_j(\alpha) \;=\; \tilde{\theta}_2(\alpha) \;=\; (\alpha - \delta_p(\xi_2;\tilde{\mathcal{C}}))/(S(\tilde{\mathcal{C}})+1) \;=\; (\alpha-\tau-se_1)/(e_*+1).$$

The estimate (3) or (4) in this case remains unchanged

$$|S(\tilde{\phi};p^\alpha)| \;\le\; 3p^2 p^{-(\alpha-\tau-se_1)/(e_2+e_3+1)},$$

illustrating the stability of the estimate.

1.4. **A generalisation.** As the proof of Theorem 1.1 is elementary, it lends itself to generalisation. Let $\mathfrak{o}$ be any ring endowed with a discrete valuation so that $|x| \le 1$ for every $x \in \mathfrak{o}$. If $\bar{\mathfrak{o}}$ denotes the completion with respect to $|\cdot|$ with $\pi$ a prime element generating the maximal ideal, we make the finiteness assumption that the residue class field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ is finite, say with $q = p^f$ elements where $p$ is prime. The valuation $|\cdot|$ on $\mathfrak{o}$ extends uniquely to $\bar{\mathfrak{o}}$ and we take the valuation normalised so that $|\pi| = q^{-1}$. We denote by $L$ the field of fractions of $\bar{\mathfrak{o}}$ and our finiteness hypothesis on the residue class field implies that $L$ is a local field. Hence $L$ is a finite field extension of the $p$-adic field $\mathbb{Q}_p$ (in the characteristic 0 case) or the field $\mathbb{F}_p((\pi))$ of Laurent series with coefficients in the field $\mathbb{F}_p$ of integers modulo $p$ (in the positive characteristic case); in the latter case we can be more explicit, namely $L = \mathbb{F}_q((\pi))$ where $q = p^f$ is defined above as the number of elements in the residue class field. If $n$ is the degree of $L$ over $\mathbb{Q}_p$ or $\mathbb{F}_p((\pi))$, then $n = ef$ where $f$, defined above, is the residual degree and the exponent $e$ is the ramification index of this extension. In the characteristic 0 case, viewing $\mathbb{Z}$ as a subring of $\mathfrak{o}$ or $\bar{\mathfrak{o}}$, we have $p = \pi^e u$ for some unit $u$ in $\bar{\mathfrak{o}}$.

Elements $x \in \bar{\mathfrak{o}}$ have a unique power series representation $x = \sum_{j\ge 0} x_j\pi^j$ with the $x_j$ lying in a fixed set of representations of the elements of the field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$. It is easy to see that the prime element $\pi$ and representations $\{x_j\}$ in $\bar{\mathfrak{o}}$ of the residue class field of $\bar{\mathfrak{o}}$ can be chosen from the ring $\mathfrak{o}$ itself.

We identify each element $\bar{x} = x + \pi^s\mathfrak{o}$ in the factor ring $\mathfrak{o}/\pi^s\mathfrak{o}$ (which can be expressed geometrically as the ball $B_{q^{-s}}(x) := \{y \in \mathfrak{o} : |y-x| \le q^{-s}\}$ centred at $x$ with radius $q^{-s}$) with the truncated expansion $x_0 + x_1\pi + \cdots + x_{s-1}\pi^{s-1}$ of $x$, uniquely determined by $\bar{x}$. Let $\chi'$ be a non-principal additive character on the factor ring $\mathfrak{o}/\pi^\alpha\mathfrak{o}$ and $\bar{\phi}$ a polynomial with coefficients in $\mathfrak{o}/\pi^\alpha\mathfrak{o}$. With the above identifications, the character sum

$$S_\chi(\phi;\pi^\alpha) \;:=\; q^{-\alpha}\sum_{\bar{x}\in\mathfrak{o}/\pi^\alpha\mathfrak{o}} \chi'(\bar{\phi}(\bar{x})) \;=\; q^{-\alpha}\sum_{x\le\pi^\alpha}\chi(\phi(x)) \tag{6}$$

where $\chi$ is a non-principal additive character of $\mathfrak{o}$ which is equal to 1 on $\pi^\alpha\mathfrak{o}$ and $\phi \in \mathfrak{o}[X]$ (the coefficients $a_j$ of $\phi$ being some choice of representation in $\mathfrak{o}$ of the corresponding coefficient $\bar{a}_j$ of $\bar{\phi}$); here we use the nonstandard notation $\sum_{x\le\pi^\alpha}$ to indicate the finite sum over elements in $\mathfrak{o}$ of the form $x = x_0 + x_1\pi + \cdots + x_{\alpha-1}\pi^{\alpha-1}$ where each $x_j$ varies over the $q$ representations in $\mathfrak{o}$ of the elements in the residue class field.

And vice-versa. Starting with a non-principal additive character $\chi$ on $\mathfrak{o}$ which is equal to 1 on $\pi^\alpha\mathfrak{o}$ and a polynomial $\phi \in \mathfrak{o}[X]$, we could have defined $S_\chi(\phi;\pi^\alpha)$

by the right side of (6). The character $\chi$ gives rise to a unique additive character $\chi'$ on the factor ring $\mathfrak{o}/\pi^\alpha\mathfrak{o}$ so that the sums in (6) are equal. The coefficients of the polynomial $\bar{\phi}$ being reduced mod $\pi^\alpha\mathfrak{o}$ from the coefficients of $\phi$. Finally we will assume that $\chi$ or $\chi'$ is a primitive character in that there is an $x \in \mathfrak{o}$ with $|x| = q^{-\alpha+1}$ such that $\chi(x) \neq 1$. If no such $x$ exists then $\chi$ would restrict to a non-principal character on the factor ring $\mathfrak{o}/\pi^{\alpha-1}\mathfrak{o}$.

Let $\phi'(x) = a_0 \prod (x-\xi_j)^{e_j}$ be the factorisation of the derivative $\phi'$ in terms of its $m$ distinct roots $\{\xi_1, \dots, \xi_m\}$, lying in some finite field extension $K$ of $L$. Our discrete valuation $|\cdot|$ on $\mathfrak{o}$ extends uniquely to $K$ which we continue to denote by $|\cdot|$. This allows us to define $E_{q^{-\alpha}}(\xi_j; \mathcal{C})$ exactly as in (2) using the valuation $|\cdot|$ on $K$, the set $\mathcal{C} \subset \{\xi_1, \dots, \xi_m\}$ being a root cluster containing $\xi_j$. Then Theorem 1.1 extends in the following way.

**Theorem 1.5.** *Suppose we are in the above setting. If $\mathfrak{o}$ has characteristic 0, suppose that either $p >$ degree$(\phi) \geq 2$ or $p > e$. If $\mathfrak{o}$ has positive characteristic, suppose that $p >$ degree$(\phi) \geq 2$. Then*

$$|S_\chi(\phi; \pi^\alpha)| \ \leq \ m\, q^2 \max_{1 \leq j \leq m} \min_{\xi_j \in \mathcal{C}} E_{q^{-\alpha}}(\xi_j; \mathcal{C}) \tag{7}$$

*where the minimum is taken over all root clusters $\mathcal{C}$ containing $\xi_j$.*

*Remarks*:

- If the extension $L$ is unramified, then there is no restriction when the characteristic is 0 since $p$ is prime and so $p \geq 2 > 1 = e$ in this case. Hence Theorem 1.5 is a strict generalisation of Theorem 1.1. Improvements on the factor $q^2$ are also possible here; see Section 6.
- A basic example to keep in mind is a general Dedekind domain $\mathfrak{o}$ where discrete valuations arise in a natural way. To any nonzero prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ we associate a discrete valuation $\mathrm{ord}_\mathfrak{p}$ defined on $\mathfrak{o}$ so that $\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}$ is the $\mathfrak{p}$ factor in the prime ideal decomposition of the principal ideal $x\mathfrak{o}$ generated by $x \in \mathfrak{o}$. When the residue class field $\mathfrak{o}/\mathfrak{p}$ is finite, say with $q$ elements, then via the isomorphism $\mathfrak{o}/\mathfrak{p} \to \bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$, we see that the multiplicative valuation $|x| := q^{-\mathrm{ord}_\mathfrak{p}(x)}$, extended uniquely to $\bar{\mathfrak{o}}$, is automatically normalised with $|\pi| = q^{-1}$ or $\mathrm{ord}_\mathfrak{p}(\pi) = 1$.

## 2. Euclidean considerations and motivations

Here we give a quick proof of the estimate (1), reducing matters to a sublevel set estimate which can be found in [9] (in fact we will give a proof of this sublevel set estimate, in an abstract setting, in Section 4). This proof is slightly different from the one given in [8] but is more easily adapted to treating character sums. Recall that we want to bound $I_\lambda = \int e^{2\pi i \lambda \phi(x)} \psi(x) dx$ where $\phi$ is a real polynomial and $\phi'(x) = a_0 \prod (x - z_j)^{e_j}$ where $\{z_1, \dots, z_m\}$ lists the $m$ distinct roots (lying in $\mathbb{C}$) of $\phi'$. Set

$$\delta \ = \ \delta(\lambda) \ = \ \big[\lambda^{-S(\mathcal{C}^*)} |a_0 \prod_{z_k \notin \mathcal{C}^*} (z_{j_*} - z_k)^{e_k}|\big]^{1/[S(\mathcal{C}^*)+1]}$$

where $j_*$ and $\mathcal{C}^*$, a root cluster containing $z_{j_*}$, is a choice where the *max min* is attained in

$$\max_{1\leq j\leq m}\min_{z_j\in\mathcal{C}} E_\lambda(z_j;\mathcal{C}) \;=\; \max_{1\leq j\leq m}\min_{z_j\in\mathcal{C}}\Big[\frac{|\lambda|^{-1}}{|a_0\prod_{z_k\notin\mathcal{C}}(z_j-z_k)^{m_k}|}\Big]^{1/[S(\mathcal{C})+1]}.$$

For any $\delta'>0$, define

$$r(\delta') \;=\; \max_{1\leq j\leq m}\min_{z_j\in\mathcal{C}} r_{\mathcal{C},j}(\delta') \quad\text{where}\quad r_{\mathcal{C},j}(\delta') \;:=\; \Big[\frac{\delta'}{|a_0\prod_{z_k\notin\mathcal{C}}(z_j-z_k)^{m_k}|}\Big]^{1/S(\mathcal{C})}.$$

One easily checks that $r(\delta)=\max_j\min_{z_j\in\mathcal{C}}E_\lambda(z_j;\mathcal{C})$ for our $\delta=\delta(\lambda)$ defined above.

Now we simply split (we drop reference to the cut-off $\psi$ for convenience)

$$I_\lambda \;=\; \int_{\{x:|\phi'(x)|\leq\delta\}} e^{2\pi i\lambda\phi(x)}dx \;+\; \int_{\{x:|\phi'(x)|>\delta\}} e^{2\pi i\lambda\phi(x)}dx \;:=\; I+II$$

For $I$ we use the trivial estimate $|I|\leq|\{x:|\phi'(x)|\leq\delta\}|$ and this sublevel set has the desired bound $C_d\,r(\delta)$ according to Theorem 1 in [9]. For $II$, the region of integration splits into $O(d)$ intervals, and on each of these intervals, a simple integration by parts argument gives a bound $O(1/|\lambda|\delta)$ which in turn gives the desired bound from our definition of $\delta$.

The bound $O(1/|\lambda|\delta)$ obtained by integrating by parts only occurs in a small neighborhood of the set $\{x:|\phi'(x)|\leq\delta\}$, a bound which improves by continued integration by parts away from this neighborhood. The same will occur in our discrete setting for character sums $S_\chi(\phi;\pi^\alpha)$. In the next section we will see that by passing to the completion $\bar{\mathfrak{o}}$, we can represent $S_\chi$ by an "oscillatory integral" over $\bar{\mathfrak{o}}$; namely

$$S_\chi(\phi;\pi^\alpha) \;=\; \int_{\bar{\mathfrak{o}}}\psi(\pi^{-\alpha}\phi(x))\,d\mu(x)$$

for some additive character $\psi$ of the field of fractions $L$ of $\bar{\mathfrak{o}}$. We will estimate $S_\chi$ in the same way as $I_\lambda$ above by splitting $S_\chi$ as

$$\int_{\{x:|\phi'(x)|\leq\delta\}}\psi(\pi^{-\alpha}\phi(x))d\mu(x) \;+\; \int_{\{x:|\phi'(x)|>\delta\}}\psi(\pi^{-\alpha}\phi(x))d\mu(x) \;:=\; I \;+\; II$$

where $\delta=\delta(q^\alpha)$ is the analogue of $\delta(\lambda)$ in the discrete setting (formally replace $\lambda$ with $q^\alpha$ and the archimedean absolute value on $\mathbb{C}$ with the non-archimedean absolute value $|\cdot|$ in the definition for $\delta(\lambda)$ above).

Using the non-archimedean analogue of the sublevel set estimate in [9] which can be found in [11] gives the favourable bound

$$I \;\leq\; \mu(\{x:|\phi'(x)|\leq\delta\}) \;\leq\; m\max_j\min_{\mathcal{C}\ni\xi_j}E_{q^{-\alpha}}(\xi_j;\mathcal{C}).$$

For $II$ we would like to "integrate-by-parts" to achieve a bound $O(1/q^\alpha\delta)$ which matches the above bound for $I$ by the definition of $\delta$. As in the euclidean setting we might expect to get better (rapid decay) estimates as we move away from the set $\{|\phi'(x)|\leq\delta\}$. In fact in the discrete setting this expectation is quantified more

exactly; we will find a precise neighborhood $\mathcal{N}$ of $\{|\phi'(x)| \leq \delta\}$ outside of which the rapid decay is 0. That is,

$$\int_{\bar{\mathfrak{o}}\setminus\mathcal{N}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x) \;=\; 0.$$

The measure of the neighborhood $\mathcal{N}$ will satisfy $\mu(\mathcal{N}) \leq mq^2 \max_J \min_{\mathcal{C}\ni\xi_j} E_{q^{-\alpha}}(\xi_j;\mathcal{C})$, giving the desired estimate (7) in Theorem 1.5.

Improvements to this estimate are made by establishing any nontrivial bound for the integral

$$\int_{\mathcal{N}\setminus\{|\phi'(x)|\leq\delta\}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x). \tag{8}$$

Such an improvement will be discussed in Section 6.

## 3. Passing to the completion

Recall that the setting of Theorem 1.5 is a general ring $\mathfrak{o}$ with a discrete valuation $|\cdot|$ so that $|x| \leq 1$ for every $x \in \mathfrak{o}$. If $\bar{\mathfrak{o}}$ denotes the completion of $\mathfrak{o}$ with respect to $|\cdot|$ and $\pi$ a prime element, we assume that the residue class field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ is finite with $q = p^f$ elements where $p$ is prime.

It will be convenient for us to pass to the completion $\bar{\mathfrak{o}}$. This will enable us to write our character sum as an "oscillatory integral" over a local field, to write the number of solutions to a polynomial congruence as the measure of a sublevel set, etc... This allows us in turn to carry over heuristics from the euclidean setting more easily. Since the residue class field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ is finite, the ring $\bar{\mathfrak{o}}$ is then the compact ring of integers of the local field $L$, the quotient field of $\bar{\mathfrak{o}}$. We then have at our disposal a Haar measure $d\mu$ on $L$ which we normalise so that $\mu(\bar{\mathfrak{o}}) = 1$. The discrete valuation $|\cdot|$, initially defined on $\mathfrak{o}$, extends uniquely to a valuation on $L$ which we continue to denote by $|\cdot|$.

Let us start with solutions to a polynomial congruence $g \equiv 0 \bmod \pi^s\mathfrak{o}$ where $g \in \mathfrak{o}[X]$. By a solution we mean an element $\bar{x} = x + \pi^s\mathfrak{o}$ in the factor ring $\mathfrak{o}/\pi^s\mathfrak{o}$ where $g(x) \in \pi^s\mathfrak{o}$. We use the notation $N(g;\pi^s) = q^{-s}\#\{g \equiv 0 \bmod \pi^s\mathfrak{o}\}$ to denote the normalised number of solutions to this congruence. Passing to the completion $\bar{\mathfrak{o}}$, the number of solutions, considered now as elements $\bar{x} = x + \pi^s\bar{\mathfrak{o}}$ in the factor ring $\bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}$, remains the same. We have

$$N(g;\pi^s) \;=\; \mu\big(\{z \in \bar{\mathfrak{o}} :\; |g(z)| \;\leq\; q^{-s}\}\big). \tag{9}$$

In fact the right hand side of (9) is equal to

$$\int_{\bar{\mathfrak{o}}} \mathbf{1}_{\{|g(z)|\leq q^{-s}\}}(y)\, d\mu(y) \;=\; \sum_{x' \leq \pi^s\bar{\mathfrak{o}}} \int_{B_{q^{-s}}(x')} \mathbf{1}_{\{|g(z)|\leq q^{-s}\}}(y)\, d\mu(y)$$

$$=\; q^{-s}\#\{x' \leq \pi^s\bar{\mathfrak{o}} :\; |g(x')| \;\leq\; q^{-s}\} \;=\; N(g;\pi^s).$$

Here $B_r(z) = \{y \in L : |y - z| \leq r\}$ denote balls in $L$ arising from the valuation $|\cdot|$ and the second equality follows since $|g(y)| \leq q^{-s}$ if and only if $|g(x')| \leq q^{-s}$ for elements $y \in B_{q^{-s}}(x')$. Recall the nonstandard notation $x' \leq \pi^s\bar{\mathfrak{o}}$ we are using to

indicate the elements of the form $x' = x_0 + x_1\pi + \cdots + x_{s-1}\pi^{s-1}$ where each $x_j$ varies over the $q$ representations in $\mathfrak{o}$ of the elements in the residue class field.

A similar identity holds for character sums. Starting with a non-principal additive character $\chi$ on $\mathfrak{o}$ with $\chi \equiv 1$ on $\pi^\alpha\mathfrak{o}$ and a polynomial $\phi \in \mathfrak{o}[X]$ defining the character sum $S_\chi(\phi;\pi^\alpha)$, we can find a non-principal additive character $\psi$ on $L$ with $\psi \equiv 1$ on $\bar{\mathfrak{o}}$ so that

$$S_\chi(\phi;\pi^\alpha) \;=\; \int_{\bar{\mathfrak{o}}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x). \tag{10}$$

Furthermore if $\chi$ is a primitive character, then $\psi$ above will also be non-trivial on $\{z \in L : |z| \le q\}$. In fact $\chi$ lifts to a non-principal character $\bar\chi$ on $\bar{\mathfrak{o}}$ which is equal to 1 on $\pi^\alpha\bar{\mathfrak{o}}$. The characters of $\bar{\mathfrak{o}}$ arise as $x \to \psi_0(yx)$ for some $y = \sum_{j=-m}^{-1} x_j\pi^j$ and some fixed non-principal character $\psi_0$ on $L$ which is 1 on $\bar{\mathfrak{o}}$ and non-trivial on $\{z \in L : |z| \le q\}$. Hence $\bar\chi(x) = \psi_0(y'x)$ for some $y'$ satisfying $|y'| = q^\alpha$. In fact since $\psi_0$ is non-trivial on $B_q(0)$ we can find an $x$ with $|y'x| = q$ so that $\bar\chi(x) \ne 1$ and hence $|x| \ge q^{-\alpha+1}$ implying $|y'| \le q^\alpha$. On the other hand since $\chi$ is a primitive character, we can find a $v$ with $|v| = q^{-\alpha+1}$ so that $\psi_0(y'v) = \bar\chi(v) \ne 1$. This implies that $|y'|q^{-\alpha+1} = |y'v| \ge q$ and so $|y'| \ge q^\alpha$.

Therefore the character $\psi(z) := \psi_0(y'\pi^\alpha z)$ on $L$ has the properties $\psi(\pi^{-\alpha}x) = \bar\chi(x)$ on $\bar{\mathfrak{o}}$, $\psi \equiv 1$ on $\bar{\mathfrak{o}}$ and $\psi$ is non-trivial on $B_q(0)$. Furthermore

$$\int_{\bar{\mathfrak{o}}} \psi(\pi^{-\alpha}\phi(y))d\mu(y) = \sum_{x' \le \pi^\alpha\bar{\mathfrak{o}}} \int_{B_{q^{-\alpha}}(x')} \psi(\pi^{-\alpha}\phi(y))d\mu(y) = \sum_{x' \le \pi^\alpha\bar{\mathfrak{o}}} \psi(\pi^{-\alpha}\phi(x'))$$

$$= \; q^{-\alpha} \sum_{x' \le \pi^\alpha\bar{\mathfrak{o}}} \bar\chi(\phi(x')) \;=\; q^{-\alpha} \sum_{x \le \pi^\alpha\mathfrak{o}} \chi(\phi(x)) \;=\; S_\chi(\phi;\pi^\alpha)$$

which establishes (10).

## 4. Polynomial congruences and sublevel sets

In [11] a sharp bound for the number of solutions to general polynomial congruences was proved which will play a key role in the proof of Theorem 1.1 and Theorem 1.5. This bound relies on the following structural statement about sublevel sets for polynomials which is valid in any ring $A$ with a valuation $|\cdot|$, not necessarily discrete. Since the proof is elementary and short we reproduce it for the convenience of the reader.

**Proposition 4.1.** [11] *Suppose $A$ is a commutative ring with a valuation $|\cdot|$ and let $P(x) = a_0\prod(x-\xi_j)^{e_j}$ be a polynomial in $A[X]$ with distinct roots $\xi_1,\dots,\xi_m$ lying in some field extension $K$. Then*

$$\big\{x \in A :\; |P(x)| \le \delta\big\} \;=\; \bigcup_{j=1}^{m} [B_{r_j}(\xi_j) \cap A] \tag{11}$$

*Here*

$$r_j \;=\; \min_{\mathcal{C} \ni \xi_j} r_{\mathcal{C},j}(\delta) \;=\; \min_{\mathcal{C} \ni \xi_j} \Big[\frac{\delta}{|a_d \prod_{\xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k}|}\Big]^{1/S(\mathcal{C})}$$

*where the minimum is taken over all root clusters $\mathcal{C}$ containing $\xi_j$. Also $B_r(z) = \{y \in K : |y-z| \le r\}$ is the 'ball' centred at $z \in K$ with radius $r$ where the valuation $|\cdot|$ on $K$ is any extension of the original valuation on $A$.*

*Remark*: Proposition 4.1 is a slight extension of a result of Phong, Stein and Sturm [9] where an upper bound on the measure of polynomial sublevel sets is given when $A = \mathbb{R}$. However their argument gives an upper set inclusion in (11) in the setting of the reals. As the proof below will show, there is an analogous statement of Proposition 4.1 valid in archimedean settings as well ($\mathbb{R}$ or $\mathbb{C}$ for example) but then the equality of sets is replaced by two set inclusions and a few factors of 2 appear in the definition of $r_{\mathcal{C},j}$.

**Proof** This will be done by establishing two set inclusions. Set $A_j := \{x \in A : |x - \xi_j| = \min_k(|x - \xi_k|)\}$ and note that

$$\big\{x \in A : |P(x)| \le \delta\big\} \ \subset \ \bigcup_{j=1}^{m} \big\{x \in A_j : \ |P(x)| \le \delta\big\}.$$

Now fix $j$, $1 \le j \le m$, and observe that when $x \in A_j$,

$$|P(x)| \ \ge \ \big|a_0 \prod_{\xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k}\big| \cdot \big|\prod_{\xi_k \in \mathcal{C}} (x - \xi_k)^{e_k}\big|$$

for any cluster $\mathcal{C}$ containing $\xi_j$ since $|\xi_j - \xi_k| \le \max(|\xi_j - x|, |x - \xi_k|) = |x - \xi_k|$ when $x \in A_j$. Therefore for $x \in A_j$, if also $|P(x)| \le \delta$, then

$$|x - \xi_j|^{S(\mathcal{C})} \ \le \ |\prod_{\xi_k \in \mathcal{C}} (x - \xi_k)^{e_k}| \ \le \ r_{\mathcal{C},j}^{S(\mathcal{C})}$$

for any cluster $\mathcal{C}$ containing $\xi_j$ and this gives

$$\big\{x \in A_j : |P(x)| \le \delta\big\} \ \subset \bigcap_{\mathcal{C}: \xi_j \in \mathcal{C}} \big[B_{r_{\mathcal{C},j}}(\xi_j) \cap A\big] \ = \ B_{r_j}(\xi_j) \cap A,$$

establishing the first set inclusion.

For the second set inclusion, if $x$ lies in the set on the right in (11), then there is a $j$, $1 \le j \le m$, so that $x \in B_{r_j}(\xi_j) = \cap_{\xi_j \in \mathcal{C}} B_{r_{\mathcal{C},j}}(\xi_j)$ where the intersection is taken over all root clusters $\mathcal{C}$ containing $\xi_j$. Next we consider a particular cluster containing $\xi_j$, depending on $x$; namely

$$\mathcal{C}_x \ := \ \{\xi_k : \ |\xi_j - \xi_k| \le |x - \xi_j|\}$$

and so in particular $|x - \xi_j| \le r_{\mathcal{C}_x,j}$. Therefore

$$|P(x)| \ = \ \big|a_0 \prod_{\xi_k \notin \mathcal{C}_x} (\xi_j - \xi_k)^{e_k}\big| \, \big|\prod_{\xi_k \in \mathcal{C}_x} (x - \xi_k)^{e_k}\big|$$

since $|x - \xi_k| = |\xi_k - \xi_j + \xi_j - x| = |\xi_k - \xi_j|$ for $\xi_k \notin \mathcal{C}_x$. On the other hand, when $\xi_k \in \mathcal{C}_x$, $|x - \xi_k| \le \max(|x - \xi_j|, |\xi_j - \xi_k|) = |x - \xi_j|$ and hence

$$|P(x)| \ \le \ \big|a_0 \prod_{\xi_k \notin \mathcal{C}_x} (\xi_j - \xi_k)^{e_k}\big| \, |x - \xi_j|^{S(\mathcal{C}_x)} \ \le \ \delta$$

since, as we observed earlier, $|x - \xi_j| \le r_{\mathcal{C}_x,j}$. This completes the proof of the proposition. ∎

Returning to our setting of a subring $\mathfrak{o}$ of the ring of integers of a discrete valuation $|\cdot|$ whose residue class field $\mathfrak{o}/\pi\mathfrak{o}$ is finite, we now give a simple proof of the result in [11] on the number $N(f;\pi^s)$ of solutions to a polynomial congruence $f \equiv 0 \mod \pi^s\mathfrak{o}$. The bounds on $N(f;\pi^s)$ are most conveniently expressed in terms of the additive form $\mathrm{ord}(x) = -\log_q(|x|)$ (so that $|x| = q^{-\mathrm{ord}(x)}$) of the valuation. Given a polynomial $f(x) = a_0\prod(x-\xi_j)^{e_j} \in \mathfrak{o}[X]$ whose $m$ distinct roots $\{\xi_1,\dots,\xi_m\}$ lie in $K$, a finite field extension of the field of fractions $L$ of the completion $\bar{\mathfrak{o}}$ with respect to $|\cdot|$. Our valuation extends uniquely to $K$ and we continue to denote the valuation for $y \in K$ as $|y|$ or $\mathrm{ord}(y)$.

For each root $\xi_j$ and root cluster $\mathcal{C}$ containing $\xi_j$, we define

$$\delta(\xi_j;\mathcal{C}) \;:=\; \mathrm{ord}\big(a_0 \prod_{k:\xi_k\notin\mathcal{C}} (\xi_j-\xi_k)^{e_k}\big)$$

and

$$\vartheta_j \;=\; \vartheta_j(s) \;:=\; \max_{\xi_j\in\mathcal{C}} \frac{(s-\delta(\xi_j;\mathcal{C}))}{S(\mathcal{C})}$$

where the maximum is taken over all root clusters $\mathcal{C}$ containing the root $\xi_j$. Recall $S(\mathcal{C}) = \sum_{k:\xi_k\in\mathcal{C}} e_k$. We pick out a special set of indices $\mathcal{I} := \{1 \le j \le m : B_{q^{-\vartheta_j}}(\xi_j)\cap\mathfrak{o} \neq \emptyset\}$ where we continue to use the ball notation $B_r(z) = \{y\in K : |y-z|\le r\}$.

**Theorem 4.2.** [11] *With the notation as above, if* $\min_{j\in\mathcal{I}}\vartheta_j \le s$, *we have*

$$q^{-\min_{j\in\mathcal{I}}\vartheta_j - 1} \;\le\; N(f;\pi^s) \;\le\; m\, q^{-\min_{j\in\mathcal{I}}\vartheta_j} \tag{12}$$

*where the minimum* $\min_{j\in\mathcal{I}}\vartheta_j$ *is interpreted as* $\infty$ *if* $\mathcal{I}=\emptyset$.

**Proof** From the discussion in Section 3 it suffices to pass to the completion $\bar{\mathfrak{o}}$ and establish the bounds

$$q^{-\min_{j\in\mathcal{I}}\vartheta_j - 1} \;\le\; \mu\big(\{z\in\bar{\mathfrak{o}} : |f(z)|\le q^{-s}\}\big) \;\le\; m\, q^{-\min_{j\in\mathcal{I}}\vartheta_j}. \tag{13}$$

From Proposition 4.1 we have

$$\{z\in\bar{\mathfrak{o}} : |f(z)|\le q^{-s}\} \;=\; \bigcup_{j=1}^{m} [B_{r_j}(\xi_j)\cap\bar{\mathfrak{o}}] \tag{14}$$

where

$$r_j \;=\; \min_{\mathcal{C}\ni\xi_j} r_{\mathcal{C},j}(q^{-s}) \;=\; \min_{\mathcal{C}\ni\xi_j} \Big[\frac{q^{-s}}{|a_0\prod_{\xi_k\notin\mathcal{C}}(\xi_j-\xi_k)^{e_k}|}\Big]^{1/S(\mathcal{C})} \;=\; q^{-\vartheta_j(s)}.$$

We note that by the non-archimedean nature of $|\cdot|$, we have $\mathcal{I} = \{1\le j\le m : B_{r_j}(\xi_j)\cap\bar{\mathfrak{o}}\neq\emptyset\}$. We will need to estimate $\mu(B_r(\xi)\cap\bar{\mathfrak{o}})$. Again by the non-archimedean property of $|\cdot|$, if $B_r(\xi)\cap\bar{\mathfrak{o}}\neq\emptyset$, we can find a $y\in\bar{\mathfrak{o}}$ so that $B_r(\xi)\cap\bar{\mathfrak{o}} = \{x\in\bar{\mathfrak{o}} : |x-y|\le r\}$. Therefore, if $q^{-t}\le r < q^{-t+1}$, we have

$$\mu\big(B_r(\xi)\cap\bar{\mathfrak{o}}\big) \;=\; q^{-t} \tag{15}$$

whenever $B_r(\xi)\cap\bar{\mathfrak{o}}\neq\emptyset$. This follows by the translation-invariance and dilation property of $\mu$ as well as our normalisation $\mu(\bar{\mathfrak{o}}) = 1$.

Hence by (15), (14) immediately gives us the upper bound in (13). For the lower bound, (14) implies that

$$\max_{j\in\mathcal{I}} \mu\big(B_{r_j}(\xi)\cap\bar{\mathfrak{o}}\big) \;\le\; \mu\big(\{z\in\bar{\mathfrak{o}} : |f(z)|\le q^{-s}\}\big)$$

and this gives the lower bound in (13) by (15). This completes our simplified proof of Theorem 4.2.

■

## 5. Controlling character sums – a general principle

In this section we give the details to our plan for bounding the character sum $S_\chi(\phi;\pi^\alpha)$ defined in (6) which was outlined in the second half of Section 2.

We begin by recalling some notation introduced previously. The distinct roots $\{\xi_1,\dots,\xi_m\}$ of $\phi'(x)=a_0\prod(x-\xi_j)^{e_j}$ lie in some field extension $K$ of the field of fractions $L$ of $\bar{\mathfrak{o}}$. Our valuation $|\cdot|$ (or ord in additive form) extends uniquely to $K$ and we define

$$E_{q^{-\alpha}}(\xi_j;\mathcal{C}) \;=\; \Big[\frac{q^{-\alpha}}{|a_0\prod_{z_k\notin\mathcal{C}}(z_j-z_k)^{e_k}|}\Big]^{1/[S(\mathcal{C})+1]} \;=\; q^{-(\alpha-\delta(\xi_j;\mathcal{C}))/(S(\mathcal{C})+1)}$$

where

$$\delta(\xi_j;\mathcal{C}) \;=\; \mathrm{ord}\big(a_0\prod_{k:\xi_k\notin\mathcal{C}}(\xi_j-\xi_k)^{e_k}\big)$$

and $\mathcal{C}\subset\{\xi_1,\dots,\xi_m\}$ is a root cluster containing $\xi_j$.

Following the discussion in Section 2 we set

$$\delta(q^\alpha)=\big[q^{-\alpha S(\mathcal{C}^*)}|a_0\prod_{\xi_k\notin\mathcal{C}^*}(\xi_{j_*}-\xi_k)^{e_k}|\big]^{1/[S(\mathcal{C}^*)+1]}=q^{-[\alpha S(\mathcal{C}^*)+\delta(\xi_{j_*};\mathcal{C}^*)]/[S(\mathcal{C}^*)+1]}$$

where $j_*$ and $\mathcal{C}^*$, a root cluster containing $\xi_{j_*}$, is a choice where the *max min* is attained in

$$\max_{1\le j\le m}\min_{\xi_j\in\mathcal{C}} E_{q^{-\alpha}}(\xi_j;\mathcal{C}) \;=\; \max_{1\le j\le m}\min_{\xi_j\in\mathcal{C}} q^{-(\alpha-\delta(\xi_j;\mathcal{C}))/(S(\mathcal{C})+1)} \;=\; q^{-\min_j\theta_j(\alpha)}.$$

Here $\theta_j(\alpha)=\max_{\mathcal{C}\ni\xi_j}(\alpha-\delta(\xi_j;\mathcal{C}))/(S(\mathcal{C})+1)$ where the maximum is taken over all root clusters $\mathcal{C}$ containing $\xi_j$.

For any $\delta'>0$, define

$$r(\delta') \;=\; \max_{1\le j\le m}\min_{\xi_j\in\mathcal{C}} r_{\mathcal{C},j}(\delta') \quad\text{where}\quad r_{\mathcal{C},j}(\delta') \;:=\; \Big[\frac{\delta'}{|a_0\prod_{\xi_k\notin\mathcal{C}}(\xi_j-\xi_k)^{e_k}|}\Big]^{1/S(\mathcal{C})}.$$

As before one checks that $r(\delta)=\max_j\min_{\xi_j\in\mathcal{C}} E_{q^{-\alpha}}(\xi_j;\mathcal{C})$ for our $\delta=\delta(q^\alpha)$ defined above. Furthermore we note that $\delta r(\delta)=q^{-\alpha}$.

From Section 3 we can find a non-principal character $\psi$ on $L$ with $\psi = 1$ on $\bar{\mathfrak{o}}$ and which is non-trivial on $B'_q(0) = \{x \in \bar{\mathfrak{o}} : |x| \leq q\}$ such that

$$S_\chi(\phi; \pi^\alpha) \;=\; \int_{\bar{\mathfrak{o}}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x).$$

We use the notation $B'$ to denote balls in $\bar{\mathfrak{o}} \subset L$ to distinguish from balls in the field extension $K$ which we denote by $B$ without the dash. In the above integral we will consider a certain neighborhood $\mathcal{N}$ of the sublevel set $\{x \in \bar{\mathfrak{o}} : |\phi'(x)| \leq \delta\}$ where $\delta = \delta(q^\alpha)$. By (11) or (14) we have

$$\{x \in \bar{\mathfrak{o}} : |\phi'(x)| \leq \delta\} \;=\; \bigcup_{j=1}^{m} [B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}}] \tag{16}$$

where $r_j = r_j(\delta) = \min_{\mathcal{C} \ni \xi_j} r_{\mathcal{C},j}(\delta)$. Let $r = r(\delta) = \max_j r_j$ and let $t$ be the integer satisfying $q^{-t} \leq r(\delta) < q^{-t+1}$. Since the estimate (7) is trivial when $q^2 r(\delta) \geq 1$, we may assume that $t \geq 3$ in what follows. We will see that this will imply that $\alpha \geq 2$.

Let $\mathcal{J}$ denote those $j$, $1 \leq j \leq m$, such that $\{x \in K : |x - \xi_j| < q^{-t+3}\} \cap \bar{\mathfrak{o}}$ is nonempty. For each $j \in \mathcal{J}$ we fix a $y_j \in \bar{\mathfrak{o}}$ in this intersection. We will assume initially that $\mathcal{J} \neq \emptyset$ and then discuss how the argument below can be modified to give the desired result in the case when $\mathcal{J} = \emptyset$.

When $\mathcal{J}$ is nonempty, our neighborhood is simply

$$\mathcal{N} \;=\; \bigcup_{j \in \mathcal{J}} B'_{q^{-t+2}}(y_j)$$

and our basic claim is

$$\int_{\bar{\mathfrak{o}} \setminus \mathcal{N}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x) \;=\; 0. \tag{17}$$

Since $\mu(\mathcal{N}) \leq mq^2 r(\delta) = mq^2 \max_j \min_{\mathcal{C} \ni \xi_j} E_{q^{-\alpha}}(\xi_j; \mathcal{C})$, the claim (17) will imply the desired estimate (7), completing the proof of Theorem 1.5 in this case. Since each $r_j \leq r < q^{-t+1} < q^{-t+3}$, we see that for each $B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}}$ arising in the sublevel decomposition (16) which is nonempty, we have $j \in \mathcal{J}$ and $B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}} \subset B'_{q^{-t+2}}(y_j)$. This shows that $\mathcal{N}$ does indeed contain the sublevel set $\{x : |\phi'(x)| \leq \delta\}$.

Our assumption that $t \geq 3$ means that $q^{-t+2} \leq q^{-1}$. Since $\mathcal{N}$ is a finite union of pairwise disjoint balls in $\bar{\mathfrak{o}}$ of radii $q^{-t+2}$, the complement $\bar{\mathfrak{o}} \setminus \mathcal{N}$ is also a finite disjoint union of balls of radii $q^{-t+2}$. For each such fixed ball $B'_{q^{-t+2}}(y)$ in this complement, we will show

$$I_y \;:=\; \int_{B'_{q^{-t+2}}(y)} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x) \;=\; 0 \tag{18}$$

from which (17) follows. We may write

$$I_y \;=\; \psi(\pi^{-\alpha}\phi(y)) q^{-t+2} \int_{|w| \leq 1} \psi(\pi^{-\alpha} g(w))\, d\mu(w)$$

where $g(w) = \phi(y + q^{t-2}w) - \phi(y)$. For any $1 \leq j \leq m$, we have

$$|y - \xi_j| \;\geq\; q^{-t+3}. \tag{19}$$

In fact when $j \notin \mathcal{J}$, we have $|x - \xi_j| \geq q^{-t+3}$ for all $x \in \bar{\mathfrak{o}}$ and in particular (19) holds in this case. For $j \in \mathcal{J}$, (19) will follow from $|y - y_j| \geq q^{-t+3}$ which in turn follows since $B'_{q^{-t+2}}(y) \cap B'_{q^{-t+2}}(y_j) = \emptyset$. In fact since $|y_j - \xi_j| < q^{-t+3}$, we have

$$|y - \xi_j| \;=\; |y - y_j + y_j - \xi_j| \;=\; |y - y_j| \;\geq\; q^{-t+3},$$

establishing (19) in this case as well.

For $z \in B'_{q^{-t+2}}(y)$, we have $|z - \xi_j| = |y - \xi_j + z - y| = |y - \xi_j|$ which follows from (19) since $|y - \xi_j| \geq q^{-t+3} > q^{-t+2} \geq |z - y|$. This implies that

$$|\phi'(z)| \;=\; |a_0 \prod (z - \xi_j)^{e_j}| \;=\; |a_0 \prod (y - \xi_j)^{e_j}| \;=\; |\phi'(y)|$$

is constant for $z \in B'_{q^{-t+2}}(y)$. Hence $|g'(w)| = q^{-t+2}|\phi'(y + q^{t-2}w)|$ is constant for $|w| \leq 1$. Since $y \notin \mathcal{N}$ and $\mathcal{N}$ contains the sublevel set $\{x : |\phi'(x)| \leq \delta\}$, we have $|\phi'(y)| > \delta$ and so $|g'(0)| = q^{-t+2}|\phi'(y)| > q\delta r(\delta) = q^{-\alpha+1}$. As observed above, $|g'(w)|$ is constant as $w$ varies over $|w| \leq 1$ and so if we define $\sigma$ by $q^{-\sigma} = |g'(0)| = |g'(w)|$, then $\sigma \leq \alpha - 2$.

The polynomial $g(w) = a_1 w + a_2 w^2 + \ldots + a_d w^d$ has no constant term and $|a_1| = |g'(0)| = q^{-\sigma}$. Momentarily we will use our hypothesis that $p > d$ or $p > e$ in the characteristic 0 case (in the positive characteristic case we require $p > d$) to show that $|a_k| \leq |a_1|$ for all $k \geq 1$. This will allow us to consider the polynomial $f := \pi^{-\sigma} g \in \bar{\mathfrak{o}}[X]$ with the property $|f'(w)| = 1$ for all $|w| \leq 1$ and write

$$I_y \;=\; \psi(\pi^{-\alpha}\phi(y)) q^{-t+2} \int_{|w| \leq 1} \psi(\pi^{-(\alpha-\sigma)} f(w))\, d\mu(w).$$

The integral on the right vanishes since it can be decomposed as

$$\int_{|w| \leq 1} \psi(\pi^{-(\alpha-\sigma)} f(w)) d\mu(w) \;=\; \sum_{z \leq \pi^{s-1}} \int_{B'_{q^{-s+1}}(z)} \psi(\pi^{-s} f(u)) d\mu(u)$$

where $s = \alpha - \sigma \geq 2$. From the facts that $s \geq 2$ and $\psi = 1$ on $B'_1(0)$ it follows, by writing $u = z + \pi^{s-1} w$ with $|w| \leq 1$ and expanding $f(u) = f(z) + f'(z)\pi^{s-1} w + O(\pi^{2s-2})$, that $\psi(\pi^{-s} f(u)) = \psi(\pi^{-s} f(z)) \psi(\pi^{-1} f'(z) w)$. Hence each integral in the above sum is equal to

$$\psi(\pi^{-s} f(z)) q^{-s+1} \int_{|w| \leq 1} \psi(\pi^{-1} f'(z) w) d\mu(w)$$

which vanishes since $\widetilde{\psi}(w) := \psi(\pi^{-1} f'(z) w)$ is a non-principal additive character on the compact ring $B'_1(0)$. Here we use the facts that $|f'(z)| = 1$ for each $z$ and $\psi$ is non-trivial on $B'_q(0)$.

It remains to show that $|a_k| \leq |a_1|$ for each coefficient of $g$. Since $g^{(k)}(0) = (q^{-t+2})^k \phi^{(k)}(y)$ and $\phi^{(k)}(y)$ is a finite sum of terms of the form $m\phi'(y)/\prod(y - \xi_{j_\ell})$ where $m \in \mathbb{N}$ and the product is a $(k-1)$-fold product of factors $y - \xi_j$, each having a bound $|y - \xi_{j_\ell}| \geq q^{-t+3}$ by (19), the non-archimedean nature of $|\cdot|$ implies that

$$|g^{(k)}(0)| \;\leq\; \Big(\frac{q^{-t+2}}{q^{-t+3}}\Big)^{k-1} |g'(0)| \;\leq\; q^{-k+1}|g'(0)| \;=\; q^{-k+1}|a_1|. \tag{20}$$

However $k!a_k = g^{(k)}(0)$. First consider the positive characteristic case where our hypothesis is $p > d$. Then $\bar{\mathfrak{o}} = \mathbb{F}_q[[\pi]]$ is the ring of power series in $\pi$ with coefficients in $\mathbb{F}_q$ and $q = p^f$. An element $x \in \mathbb{F}_q[[\pi]]$ satisfies $|x| = q^{-m}$ if and only if $x = x_m\pi^m + x_{m+1}\pi^{m+1} + \cdots$ with $x_m \neq 0$. In this case if $j \in \mathbb{N}$ and $p \not| j$, then $jx = jx_m\pi^m + \cdots$ with $|jx| = |x|$. Hence for any $k \leq d$, we have $p \not| k!$ and so $|a_k| = |k!a_k| = |g^{(k)}(0)| \leq |a_1|$.

Turning now to the case where $\mathfrak{o}$ has characteristic 0, our hypothesis is less restrictive; requiring either $p > d$ or $p > e$. If $p^\theta \| k!$, we have $|k!| = q^{-e\theta}$ where $e$ is the ramification index. Therefore if $p > d$, then $\theta = 0$ from which $|a_k| = |k!a_k| \leq |a_1|$ as before. Now suppose $p \leq d$ but $p \geq e + 1$. Then from

$$\theta \;=\; \lfloor k/p \rfloor + \lfloor k/p^2 \rfloor + \cdots \;<\; k/(p-1),$$

we have $e\theta < ke/(p-1)$ which in turn is less than or equal to $k$ exactly when $e + 1 \leq p$. Hence $e\theta \leq k - 1$ implying that $|a_k| \leq q^{-k+1+e\theta}|a_1| \leq |a_1|$. Therefore in all cases, $|a_k| \leq |a_1|$ for every $k \geq 1$.

Finally we discuss the case when $\mathcal{J} = \emptyset$. In this case we have for each $1 \leq j \leq m$, $|x - \xi_j| \geq q^{-t+3}$ for all $x \in \bar{\mathfrak{o}}$. Let $\mathcal{I}$ denote the set of indicies $1 \leq j \leq m$ for which $B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}} \neq \emptyset$. For each $j \in \mathcal{I}$ we fix a $y_j$ in this intersection so that $B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}} = B'_{r_j}(y_j)$. Our modified neighborhood is $\mathcal{N} = \cup_{j\in\mathcal{I}} B'_{q^{-t+2}}(y_j)$ which is the empty set if $\mathcal{I} = \emptyset$. We still have

$$\mu(\mathcal{N}) \;\leq\; mq^2 r(\delta) \;=\; mq^2 \max_j \min_{\mathcal{C}\ni\xi_j} E_{q^{-\alpha}}(\xi_j; \mathcal{C})$$

and the desired result will follow if (17) holds with the modified neighborhood $\mathcal{N}$. Now one can run the argument above to establish (17) in this case using the key fact that $|x - \xi_j| \geq q^{-t+3}$ (which now automatically holds for all $x \in \bar{\mathfrak{o}}$) to show the constancy of $|\phi'(x)|$ over all balls of radius $q^{-t+2}$ in the complement $\bar{\mathfrak{o}} \setminus \mathcal{N}$ (or over all balls of radius $q^{-t+2}$ in $\bar{\mathfrak{o}}$ in the case that $\mathcal{I}$ is empty) and that the estimate (20) still holds.

## 6. A slight improvement

In this section we modify the argument in the previous section, using the estimates of A. Weil for character sums over finite fields, to give a slight improvement; namely we reduce the factor $q^2$ to $q^{3/2}$. One can make further improvements.

We continue to use the notation employed in the previous section. We may assume that $t \geq 2$; otherwise the trivial estimate for $S_\chi(\phi; \pi^\alpha)$ suffices. We begin with the case that the index set $\mathcal{J}$ is nonempty. In this case we still have the basic claim (17) from the previous section. Note that (17) trivially holds in the case $t = 2$ since then $\mathcal{N} = \bar{\mathfrak{o}}$ as $\mathcal{J}$ is assumed to be nonempty. Hence the original oscillatory integral representing our character sum is equal to

$$\int_{\mathcal{N}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x) \;=\; S_\chi(\phi; \pi^\alpha). \tag{21}$$

Instead of estimating this integral trivially by $\mu(\mathcal{N})$ as we did in the previous section, one can look for improvements by providing any nontrivial estimate for the

integral (8) mentioned at the end of Section 2. A naive way of doing this is the following.

Let $\mathcal{K}$ denote those indicies $1 \le k \le m$ such that $\{x \in K : |x-\xi_k| < q^{-t+2}\} \cap \bar{\mathfrak{o}} \neq \emptyset$ and for each $k \in \mathcal{K}$ choose a $z_k$ in this intersection. We note that $\mathcal{J} \subset \mathcal{K}$ (and so, in particular, $\mathcal{K}$ is not empty in the present case) and therefore $\mathcal{M} \subset \mathcal{N}$ where

$$\mathcal{M} \ := \ \bigcup_{k \in \mathcal{K}} B'_{q^{-t+1}}(z_k).$$

This is still a neighborhood of $\{x \in \bar{\mathfrak{o}} : |\phi'(x)| \le \delta\}$ since $B_{r_k}(\xi_k) \cap \bar{\mathfrak{o}} \subset B'_{q^{-t+1}}(z_k)$ for every $k \in \mathcal{K}$. When $k \notin \mathcal{K}$, $B_{r_k}(\xi_k) \cap \bar{\mathfrak{o}} = \emptyset$.

For each ball $B'_{q^{-t+1}}(y)$ in the complement $\mathcal{N} \setminus \mathcal{M}$ we will estimate the integral

$$I_y \ := \ \int_{B'_{q^{-t+1}}(y)} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x)$$

by $|I_y| \le (d-1)q^{-t}q^{1/2} \le (d-1)q^{1/2}r(\delta)$ using the A. Weil estimate. Since there are at most $mq$ such balls and since $\mu(\mathcal{M}) \le mq^{-t+1} \le mqr(\delta)$, we have by (21)

$$|S_\chi(\phi;\pi^\alpha)| \ \le \ mqr(\delta)[(d-1)\sqrt{q}+1] \ \le \ 2(d-1)^2 q^{3/2} r(\delta),$$

the claimed bound.

We can write the integral $I_y$ as

$$\psi(\pi^{-\alpha}\phi(y))q^{-t+1} \int_{|w|\le 1} \psi(\pi^{-\alpha}g(w))d\mu(w)$$

where now $g(w) = \phi(y+q^{t-1}w) - \phi(y)$. Arguing as in the previous section we see that $|g'(w)| = |g'(0)|$ for all $|w| \le 1$ which follows from the fact that for all $z \in B'_{q^{-t+1}}(y)$, $|z-\xi_j| = |y-\xi_j| \ge q^{-t+2}$ for every $1 \le j \le m$. Furthermore we have $\sigma \le \alpha - 1$ where $q^{-\sigma} = |g'(0)|$ and $|a_k| \le |a_1|$ for all the coefficients $a_k$ of $g$.

As before we can then write

$$I_y \ = \ \psi(\pi^{-\alpha}\phi(y))q^{-t+1} \int_{|w|\le 1} \psi(\pi^{-(\alpha-\sigma)}f(w))\, d\mu(w)$$

where $f = \pi^{-\sigma}g \in \bar{\mathfrak{o}}[X]$ and this integral vanishes if $\sigma \le \alpha - 2$. This leaves the case when $\sigma = \alpha - 1$ and here $I_y$ can be written as a character sum over the finite field $\mathfrak{o}/\pi\mathfrak{o}$ so that we can apply the A. Weil estimate $|I_y| \le (d-1)q^{-t}q^{1/2}$. This gives the slightly improved bound claimed above in the case $\mathcal{J} \neq \emptyset$.

Now suppose that $\mathcal{J}$ is empty. Here we proceed exactly as in the previous section, introducing the same set of indicies $\mathcal{I}$ and for each $j \in \mathcal{I}$, a point $y_j \in B_{r_j}(\xi_j) \cap \bar{\mathfrak{o}}$. From the previous section we have

$$\int_{\bar{\mathfrak{o}}\setminus\mathcal{N}} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x) \ = \ 0$$

where $\mathcal{N} = \cup_{j\in\mathcal{I}} B'_{q^{-t+2}}(y_j)$. One simply proceeds exactly as before to see that we can bound the integral

$$I_y \;:=\; \int_{B'_{q^{-t+1}}(y)} \psi(\pi^{-\alpha}\phi(x))\, d\mu(x)$$

by $|I_y| \le (d-1)q^{-t}q^{1/2} \le (d-1)q^{1/2}r(\delta)$ for every ball $B'_{q^{-t+1}}(y)$ in $\mathcal{N}\backslash\cup_{j\in\mathcal{I}} B'_{q^{-t+1}}(y_j)$. From this, the same estimate for $S_\chi(\phi;\pi^\alpha)$ as above follows. We leave the details to the reader.

## 7. A final remark - an estimate of Hua

In [3] an estimate on the number of 'global' solutions to a polynomial congruence was given, generalising a result of Hua on the number of classical solutions to a polynomial congruence. In exactly the same way, using the arguments from the previous sections and an elementary combinatorial inequality found in [3], one can prove the following global oscillatory integral estimate: suppose that $\phi(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x \in \mathbb{Z}[X]$ has degree at least 2. Then, uniformly in $R > 0$,

$$\Big|\int_{\{x\in\mathbb{Q}_p : |x|\le R\}} \psi(p^{-\alpha}\phi(x))\, d\mu(x)\Big| \;\le\; mp^2 p^{-\alpha/d} \tag{22}$$

whenever $p > d$ and $p \not| a_{d-k}$ for some $k \le (d-1)/2$. This estimate can fail if the smallest such $k$ is larger than $(d-1)/2$. If $R = 1$ the oscillatory integral above reduces to the complete exponential sum $S(\phi;p^\alpha)$.

Finally we come back to the discussion of Hua's estimate $|S(\phi;p^\alpha)| \le C_d p^{-\alpha/d}$ in the remarks following the statement of Theorem 1.1. The estimate of Hua holds whenever $gcd(a_d,\dots,a_1,p^\alpha) = 1$. An analogous estimate holds in the setting of Theorem 1.5. The combinatorial inequality in [3] mentioned above can be used to show that

$$\max_{1\le j\le m} \min_{\xi_j\in\mathcal{C}} E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \;\le\; p^{-\alpha/d}$$

if $p \not| a_{d-k}$ for some $k \le (d-1)/2$; furthermore this estimate fails in general. However if the maximum above is taken only over those $j$ such that $|\xi_j| \le 1$, then the estimate always holds. In fact we have

**Lemma 7.1.** *If $p > d$, and $gcd(a_d,\dots,a_1,p^\alpha) = 1$, then*

$$\max_{j:|\xi_j|\le 1} \min_{\mathcal{C}:\xi_j\in\mathcal{C}} E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \;\le\; p^{-\alpha/d}. \tag{23}$$

As remarked earlier, the proof of Theorem 1.1 (and Theorem 1.5) remains valid if the maximum in (3) or (7) is taken only over those $j$ such that $|\xi_j| \le 1$.

**Proof** If $\phi'(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$ where $n = d-1$, suppose that $p \not| b_k$ for some $0 \le k \le n$ and $p|b_j$ for all $j < k$. As mentioned earlier, if $k = 0$, we can use the cluster $\mathcal{C} = \{\xi_1,\dots,\xi_m\}$ of all roots to verify (23) in this case. Hence we may suppose that $k \ge 1$. In this case we will verify that for each $j$ such that $|\xi_j| \le 1$,

$$\min_{\mathcal{C}:\xi_j\in\mathcal{C}} E_{p^{-\alpha}}(\xi_j;\mathcal{C}) \;\le\; p^{-\alpha/d} \tag{24}$$

holds. Without loss of generality suppose that $j = 1$; in particular, $|\xi_1| \le 1$. Let us enumerate $\{y_1, \dots, y_n\}$ the roots of $\phi'$ with multiplicities such that $y_1 = \xi_1$ (so $|y_1| \le 1$).

To establish (24) (for $j = 1$) we use an elementary observation from [3]; namely,

$$\min_{\mathcal{C}:\xi_1\in\mathcal{C}}\Big[\frac{p^{-\alpha}}{|b_0\prod_{\xi_k\notin\mathcal{C}}(\xi_1-\xi_k)^{e_k}|}\Big]^{1/S(\mathcal{C})+1} \;=\; \min_{L:1\in L}\Big[\frac{p^{-\alpha}}{|b_0\prod_{\ell\notin L}(y_1-y_\ell)|}\Big]^{1/(|L|+1)}$$

where the minimum on the right-hand side is taken over all subsets $L \subset \{1, 2, \dots, n\}$ containing 1. We define a parameter $\theta$ via $p^\theta \| b_0$ (recall that we are assuming $k \ge 1$ and so $\theta \ge 1$). Since the left-hand side is equal to the left-hand side of (24) (for $j = 1$), it suffices to prove

$$\max_{1\in L:|L|=n-k}\Big|\prod_{j\notin L}(y_1-y_j)\Big| \ge p^\theta$$

which by the non-archimedean property of $|\cdot|$ follows from

$$\Big|\sum_{1\in L:|L|=n-k}\;\prod_{j\notin L}(y_1-y_j)\Big| \;=\; p^\theta. \tag{25}$$

The sum in (25), when expanded, can be written as

$$\Big|\sum_{1\in L:|L|=n-k}\;\prod_{j\notin L}(y_1-y_j)\Big| = \sum_{m=0}^{k}(-1)^{k-m}y_1^m\sum_{2\le j_1<\cdots<j_{k-m}} y_{j_1}\cdots y_{j_{k-m}} \tag{26}$$

and we now express this in terms of the elementary symmetric polynomials in $y_1, \dots, y_n$.

If

$$S_q(X_1,\dots,X_n) \;=\; \sum_{j_1<\cdots<j_q} X_{j_1}\cdots X_{j_q}$$

denotes the $q$th elementary symmetric polynomial in $n$ variables $X_1, \dots, X_n$, then $|S_q(y_1, \dots, y_n)| = p^\theta |b_q|$ where we recall that $\theta$ is defined by $p^\theta \| b_0$. Our assumption $p \not| b_k$ means that $|S_k(y_1, \dots, y_n)| = p^\theta > 1$ and our other assumptions $p|b_j$ for all $j < k$ translate to $|S_j(y_1, \dots, y_n)| < p^\theta$.

The following identity involving elementary symmetric polynomials in $n$ variables will be useful for us. For any $1 \le q \le n$,

$$\sum_{2\le j_1<\cdots<j_q} X_{j_1}\cdots X_{j_q} \;=\; \sum_{\ell=0}^{q}(-1)^\ell X_1^\ell\, S_{q-\ell}(X_1,\dots,X_n). \tag{27}$$

By convention we set $S_0 = 1$ and when $q = n$, the left side is interpreted as 0. The identity is easily verified; to the left-hand side of (27) simply add on (and then subtract off) $q$-tuples $X_{j_1}\cdots X_{j_q}$ with $j_1 = 1$, etc... Writing the left-hand side of (27) as $S_q^{\ge 2}(X_1, \dots, X_n)$, the identity (27) can be reshuffled a bit and written as

$$S_q(X_1,\dots,X_n) \;=\; S_q^{\ge 2}(X_1,\dots,X_n) + \sum_{\ell=1}^{q}(-1)^{\ell+1}X_1^\ell S_{q-\ell}(X_1,\dots,X_n)$$

for each $1 \leq q \leq n$. When $q = n$ the sum $S_n^{\geq 2}$ is empty and interpreted as 0. Applying this when $q = k < n$ and $X_j = y_j$, $1 \leq j \leq n$, we see from our assumptions ($|y_1| \leq 1$, $|S_k(y_1, \dots, y_n)| = p^\theta$, $|S_j(y_1, \dots, y_n)| < p^\theta$ for $j < k$) and the non-archimedean nature of $|\cdot|$ that

$$|S_k(y_1, \dots, y_n)| \;=\; |S_k^{\geq 2}(y_1, \dots, y_n)| \;=\; p^\theta. \tag{28}$$

The case $k = n$ leads to a contradiction. Hence we may assume that $1 \leq k \leq n-1$. Furthermore, applying (27) for $q < k$, we see that

$$\Big| \sum_{2 \leq j_1 < \cdots < j_{k-m}} y_{j_1} \cdots y_{j_{k-m}} \Big| < p^\theta \tag{29}$$

for every $1 \leq m \leq k$. Finally, the right-hand side of (26) can be written as

$$(-1)^k S_k^{\geq 2}(y_1, \dots, y_n) + \sum_{m=1}^{k} (-1)^{k-m} y_1^m \sum_{2 \leq j_1 < \cdots < j_{k-m}} y_{j_1} \cdots y_{j_{k-m}}$$

which by (28) and (29) has valuation $|\cdot|$ equal to $p^\theta$, completing the proof of (25) and hence the lemma. ∎

## References


[1] A. Carbery, B. Stones and J. Wright, *Averages in vector spaces over finite fields*, Math. Proc. Camb. Phil. Soc. 144 no. 13 (2008), 13-27.

[2] L.K. Hua, *On an exponential sum*, J. Chinese Math. Soc. 20 (1940), 301-312.

[3] M.W. Kowalski and J. Wright, *An elementary inquality with some applications*, preprint.

[4] J.H. Loxton and R. A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. **26** (1982), 15-20.

[5] J.H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canadian Math. Bull. **28** (1985), 440-454.

[6] G. Mochenhaupt and T. Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J. 121 (2004), 35-74.

[7] R.A Smith, *Estimates for exponential sums*, Proc. Amer. Math. Soc. **79** (1980), 365-368.

[8] D.H. Phong and E.M. Stein, *Oscillatory integrals with polynomial phases*, Inventiones Math. **110** (1992), 39-62.

[9] D.H. Phong, E.M. Stein and J.A. Sturm, *On the growth and stability of real analytic functions*, Amer. J. Math **121** (1999), 519-554.

[10] J. Wright, *From oscillatory integrals and sublevel sets to polynomial congruences and character sums*, J. Geom. Anal. **21** (2011), 224-240.

[11] ———, *On polynomial congruences*, preprint.

[12] ———, *The Fourier restriction problem in rings of integers*, in preparation.



Maxwell Institute of Mathematical Sciences and the School of Mathematics, University of Edinburgh, JCMB, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland

*E-mail address*: J.R.Wright@ed.ac.uk